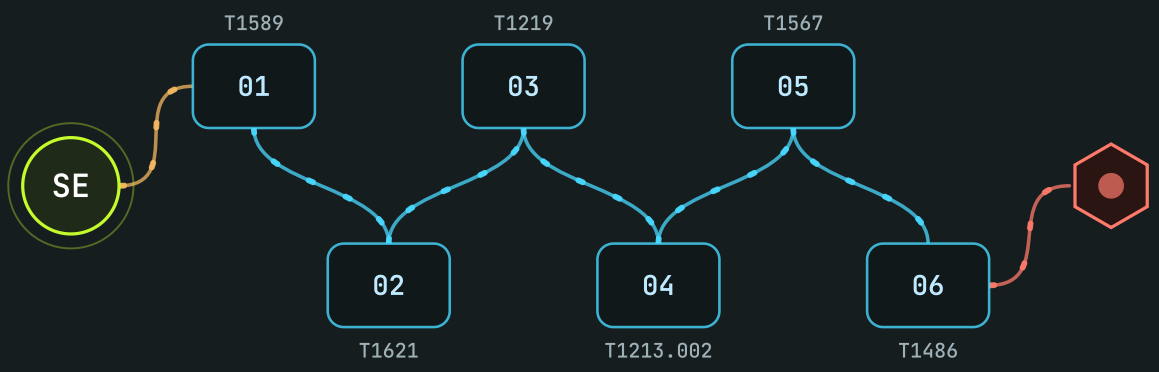


INTELLIGENCE BRIEF

Scattered Spider convictions land as the help desk playbook moves to new crews

Courts in the UK and US have sentenced Scattered Spider members and the NCA says the crew is effectively halted, but ShinyHunters-branded crews now run the same help desk vishing playbook. Harden resets and MFA now.

EDITION
Fall/Winter 2026/2027 Edition
SE-01 · Social engineering crew

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

DISRUPTED

The NCA says its action against Jubair and Flowers effectively halted the group's criminal activity and cites Microsoft's assessment that the arrests materially degraded it, while other criminals keep using the brand and its techniques. [1]

HEADLINE NUMBERS

$115M+
Ransoms the DOJ alleges victims paid, May 2022 to September 2025 [4]

5.5 yrs
Sentence each for Jubair and Flowers, July 16, 2026 [1]

12%
ShinyHunters share of Coveware's Q2 2026 extortion cases, second among actors [24]

$70M+
Extorted by ShinyHunters in 2026 so far, per the FBI [22]

KEY FACTS

INITIAL ACCESS
Help desk impersonation, phishing and smishing, push bombing, SIM swaps [13]

TARGETS
Large companies and their contracted IT help desks [13]

RANSOMWARE PARTNERS
DragonForce most recently; ALPHV/BlackCat as an affiliate from mid-2023 [13]

ALLEGED RANSOMS
More than $115 million paid, per the DOJ complaint against Jubair [4]

PROSECUTIONS
UK sentences July 2026; US pleas and sentences 2025 to 2026 [1]

SUCCESSOR CREWS
Scattered LAPSUS$ Hunters, then ShinyHunters-branded vishing and SaaS extortion [20]

02 What happened

The original edition dissected the 2023 casino intrusions, the 2024 Snowflake credential campaign and the April 2025 Marks & Spencer attack, all built on a phone call. Since then courts in the UK and US have taken guilty pleas or imposed sentences on several named members, and the FBI and CISA refreshed their advisory with 2025 tradecraft. The help desk and vishing playbook has moved to ShinyHunters-branded crews that Google tracks separately.

- Thalha Jubair and Owen Flowers pleaded guilty on June 22, 2026, the first day of trial, to a Computer Misuse Act section 3ZA offense over the August to September 2024 Transport for London attack and were each sentenced to five and a half years at Woolwich Crown Court on July 16, 2026. The NCA and CPS put TfL's losses and recovery costs at 29 million pounds, and Flowers also admitted conspiring against two US health systems, SSM Health and Sutter Health.
- A US complaint unsealed September 18, 2025 charges Jubair with computer fraud, wire fraud and money laundering conspiracies and alleges about 120 intrusions, at least 47 US victims and more than $115 million in ransoms paid between May 2022 and September 2025. The DOJ says a complaint is only an allegation and that he is presumed innocent.
- Tyler Buchanan pleaded guilty in April 2026 to conspiracy to commit wire fraud and aggravated identity theft over an SMS phishing scheme that took at least $8 million in cryptocurrency. Noah Urban was sentenced to 10 years with $13 million restitution in August 2025. The DOJ announced on July 1, 2026 that Peter Stokes, 19, was extradited from Finland and charged by complaint in Chicago over a May 2025 intrusion at a luxury jewelry retailer; he is presumed innocent.
- Connor Moucka pleaded guilty in Seattle federal court in August 2026 to computer fraud, wire fraud, aggravated identity theft and conspiracy over the 2024 Snowflake customer breaches. The DOJ cites more than 165 organizations and at least $9.5 million in victim company losses; sentencing is set for October 27, 2026 and co-defendant John Binns remained outside US custody as of the court's August 4 update.
- The joint FBI, CISA and partner advisory updated July 29, 2025 adds DragonForce ransomware on VMware ESXi, thousands of rapid Snowflake queries for exfiltration, new identities backed by fake social media profiles and rotating proxies. It also documents the actors searching Slack, Teams and Exchange Online for mentions of the intrusion and joining incident response calls.
- Scattered Lapsus$ Hunters, an alliance of Scattered Spider, LAPSUS$ and ShinyHunters personas, lost its domains to police in October 2025. In 2026 ShinyHunters-branded crews ran help desk vishing against single sign-on, scraped Salesforce Experience Cloud sites and breached an FBI recruiting site, followed by arrests in the Netherlands and the US and a reported detention in Jordan.

03 How it works

01 Build the pretext

MITRE ATT&CK T1589

Actors gather employee names, titles, managers and partial personal data, then pose as company IT or help desk staff, or as an employee calling the help desk.

02 Talk past MFA

MITRE ATT&CK T1621

Phone and SMS phishing, push bombing and SIM swaps win a password reset, a new MFA device or a one-time code without exploiting software. In January 2026 callers told employees the company was updating MFA settings, sent them to look-alike single sign-on pages and registered the attacker's own device.

03 Install remote access

MITRE ATT&CK T1219

Employees are directed to run commercial remote access tools. The actors then create new identities in the environment and back them with fake social media profiles.

04 Find the keys and listen

MITRE ATT&CK T1213.002

They search SharePoint for credential documents and watch Slack, Teams and Exchange Online for mentions of the intrusion, even joining remediation calls.

05 Pull data fast

MITRE ATT&CK T1567

Where Snowflake access exists they run thousands of queries at once to move large volumes in a short time; in 2026 campaigns the same speed was used against SharePoint, Salesforce and other SaaS.

06 Extort, then encrypt

MITRE ATT&CK T1486

Data theft for extortion comes first. In recent cases DragonForce ransomware encrypted VMware ESXi servers as a second lever.

04 Who is at risk

Any organization whose help desk can reset a password or MFA method on a phone call is exposed, and the crews that inherited the playbook now go after SaaS tenants as much as corporate networks.

- Large companies and their contracted IT help desks and outsourcers, the targets the FBI and CISA name; the M&S chairman said the point of entry also involved a third party.
- Retail, hospitality, gaming, technology, managed service providers and financial services, the sector history Microsoft documented, plus UK retailers M&S, Co-op and Harrods named in the NCA's July 2025 arrests.
- Healthcare systems: Flowers admitted conspiring against SSM Health and Sutter Health, and Krebs reports Mandiant and Google saw Oracle PeopleSoft data theft across higher education, healthcare and government.
- Salesforce customers with public Experience Cloud sites whose guest user profiles carry overly broad permissions, and Okta, Microsoft 365, Google Workspace and Snowflake tenants where one phished sign-on or one account without MFA opens the data.

Sectors in scope: Retail, Hospitality and gaming, Telecommunications and business process outsourcing, Technology and managed service providers, Financial services, Airlines and public transport, Healthcare systems, SaaS and CRM tenants (Salesforce, Snowflake, Okta, Microsoft 365).

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 UK convictions: Jubair and Flowers pleaded guilty on June 22, 2026 and were sentenced to five and a half years each on July 16, 2026 over the 29 million pound Transport for London attack of August to September 2024, which the CPS believes are the first prosecutions under section 3ZA of the Computer Misuse Act.

SOURCE 3

02 US prosecutions advanced: Stokes was extradited from Finland and charged in Chicago (announced July 1, 2026), Buchanan pleaded guilty in April 2026, Moucka pleaded guilty in August 2026, and Urban drew 10 years in August 2025. A DOJ official now puts the group at over 100 network intrusions and more than $100 million in ransom payments.

SOURCE 5

03 The FBI and CISA advisory was updated July 29, 2025 with tradecraft from investigations through June 2025: DragonForce ransomware on ESXi, rapid Snowflake exfiltration, new identities backed by fake social media profiles, proxy networks and rotating machine names.

SOURCE 13

04 The brand merged into Scattered LAPSUS$ Hunters. The alliance threatened Salesforce data it said came from 39 companies, lost its dark web and clearnet domains to police in October 2025, leaked data from six companies on October 10, 2025, and promised an extortion-as-a-service return in 2026.

SOURCE 17

05 The vishing playbook scaled up in January 2026. Google tracks three clusters (UNC6661, UNC6671 and UNC6240) in which callers posed as IT staff, sent employees to victim-branded single sign-on pages, captured credentials and MFA codes, registered their own device, then took data from Microsoft 365, Salesforce, DocuSign and Google Workspace.

SOURCE 20

06 Salesforce warned in March 2026 that a known threat actor was scraping public Experience Cloud sites through guest profiles with overly broad permissions, using a modified Mandiant scanner. ShinyHunters told The Register it took data from about 100 companies, a claim Salesforce did not confirm.

SOURCE 19

07 ShinyHunters arrests in autumn 2026: Dutch police arrested a 24-year-old man on September 15, Reuters reported a suspect known as Rey was detained and is cooperating, and the FBI arrested a Canadian ransomware negotiation executive in Pennsylvania on October 8 on a complaint alleging extortion conspiracy. The FBI says the group extorted more than $70 million so far in 2026.

SOURCE 22

08 Marks & Spencer's cost is better known: the 300 million pound figure was a projection of lost operating profit, and M&S booked 101.6 million pounds in attack costs in the half year, expects about 34 million more and received 100 million pounds in insurance proceeds.

SOURCE 15

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Require positive identity verification before any password or MFA reset on a privileged or executive account, whether the caller claims to be the employee or IT: callback to a number on file, manager approval, and video or in-person checks for admins.**

Every signature intrusion in this report began with a help desk or an employee being talked into a reset.

02 **Move privileged and remote access to phishing-resistant MFA (FIDO2 keys or passkeys) and remove SMS and push approval for admins.**

The advisory says phishing-resistant MFA resists push bombing and SIM swaps, and Google makes the same point about the 2026 vishing.

03 **Alert on any new MFA device registration, MFA method change or super admin grant shortly after a reset, and on new identities in Okta, Entra and Google Workspace.**

The actors register their own device after a vishing call and create backstopped identities to persist.

04 **Block unauthorized remote access tools with application allowlisting and alert on first use of tunneling tools such as ngrok.**

Employees are coached into installing commercial remote access software that gives the actor a foothold without malware.

05 **Audit SaaS tenants now: Salesforce connected apps and Experience Cloud guest permissions, Snowflake MFA, and stale contractor credentials.**

The 2024 Snowflake and 2026 Salesforce campaigns used valid credentials and misconfigurations, not platform flaws.

06 **Run incident response on an out-of-band channel and assume compromised Slack, Teams and email are being read.**

The advisory documents the actors joining remediation calls to learn how they are being hunted.

07 **Keep offline, tested backups of identity infrastructure and ESXi workloads.**

DragonForce encryption of ESXi is the second lever once extortion over stolen data stalls.

08 **Rehearse the vishing call with your help desk and your outsourced IT provider, then review Microsoft 365 posture and 24/7 monitoring coverage; Z7's SOC and Microsoft 365 posture review fit here.**

The attack surface is a person on a phone, and the vendor's help desk counts as yours.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

BEHAVIOR	Employee reports a call or text from 'IT' saying MFA settings are being updated, or asking them to install a remote access tool or approve an MFA prompt [20]
DOMAIN	`Look-alike single sign-on domains following the pattern <companyname>sso.com or <companyname>internal.com` [20]
BEHAVIOR	Thousands of Snowflake queries from one account in a short window, or large exports from SharePoint credential folders [13]
BEHAVIOR	New user identities created shortly after a help desk reset, with matching new social media profiles [13]

08 Sources

[1] **Two Scattered Spider Hackers Sentenced to Jail in UK** SecurityWeek · July 16, 2026. https://www.securityweek.com/two-scattered-spider-hackers-sentenced-to-jail-in-uk/

[2] **Two Scattered Spider Hackers Get 5.5 Years for Transport for London Attack** The Hacker News · July 16, 2026. https://thehackernews.com/2026/07/two-scattered-spider-hackers-get-55.html

[3] **Crown Prosecution Service statement on the sentencing of Owen Flowers and Thalha Jubair at Woolwich Crown Court** Crown Prosecution Service · July 16, 2026. https://www.cps.gov.uk/node/29855

[4] **United Kingdom National Charged in Connection with Multiple Cyber Attacks, Including on Critical Infrastructure** U.S. Department of Justice · September 18, 2025. https://justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

[5] **Alleged Member of Criminal Cyber Hacking Group Scattered Spider Arrested in Finland and Extradited to the United States** U.S. Department of Justice · July 1, 2026. https://www.justice.gov/opa/pr/alleged-member-criminal-cyber-hacking-group-scattered-spider-arrested-finland-and-extradited

[6] **Scattered Spider hacker pleads guilty to stealing $8 million in cryptocurrency** Help Net Security (reporting the DOJ release) · April 21, 2026. https://www.helpnetsecurity.com/2026/04/21/british-national-scattered-spider-guilty-sms-phishing/

[7] **Scattered Spider Hackers Plead Guilty on Day 1 of Trial** Krebs on Security · June 23, 2026. https://krebsonsecurity.com/?p=73876

[8] **Scattered Spider affiliate sentenced to 10 years in prison** The Record · August 21, 2025. https://therecord.media/scattered-spider-affiliate-sentenced-10-years

[9] **Snowflake hacker pleads guilty, faces up to 32 years in prison** Help Net Security (reporting the DOJ release) · August 6, 2026. https://www.helpnetsecurity.com/2026/08/06/snowflake-canadian-hacker-pleaded-guilty/

[10] **Snowflake Hacker Pleads Guilty Over Breach of 165+ Organizations** The Hacker News · August 6, 2026. https://thehackernews.com/2026/08/snowflake-hacker-pleads-guilty-over.html

[11] **Canadian Man Arrested in Snowflake Data Extortions** Krebs on Security · November 5, 2024. https://krebsonsecurity.com/2024/11/

[12] **UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion** Google Cloud / Mandiant · June 10, 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[13] **Joint Cybersecurity Advisory AA23-320A: Scattered Spider (updated)** FBI, CISA, RCMP, ASD's ACSC, AFP, CCCS, NCSC-UK · November 16, 2023, updated July 29, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[14] **Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction** Microsoft Threat Intelligence · October 25, 2023. https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

[15] **Marks & Spencer gets $130 million in insurance from cyberattack** Reuters via Business Insurance · November 5, 2025. https://www.businessinsurance.com/marks-spencer-gets-130-million-in-insurance-from-cyberattack/

[16] **M&S confirms social engineering led to massive ransomware attack** BleepingComputer (reporting M&S chairman's evidence to Parliament) · July 8, 2025. https://www.bleepingcomputer.com/news/security/mands-confirms-social-engineering-led-to-massive-ransomware-attack/

[17] **Scattered Lapsus$ Hunters extortion site goes dark: What's next?** CSO Online · October 14, 2025. https://www.csoonline.com/article/4072244/scattered-lapsus-hunters-extortion-site-goes-dark-whats-next.html

[18] **Scattered Lapsus$ Hunters Recruiting Women for Operations** Dataminr · February 24, 2026. https://www.dataminr.com/resources/intel-brief/slh-recruiting-women-for-vishing/

[19] **ShinyHunters claims yet another Salesforce customers breach** The Register (reporting Salesforce's advisory) · March 9, 2026. https://www.theregister.com/security/2026/03/09/shinyhunters-claims-yet-another-salesforce-customers-breach/5220118

[20] **Vishing for Access: Tracking the Expansion of ShinyHunters-Branded SaaS Data Theft** Google Cloud / Google Threat Intelligence Group · January 30, 2026. https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft

[21] **ShinyHunters Extorted Boeing Spin-off Prior to Arrests** Krebs on Security · October 7, 2026. https://krebsonsecurity.com/2026/10/shinyhunters-extorted-boeing-spin-off-prior-to-arrests/

[22] **FBI Arrests Founder of Ransomware Negotiation Firm** Krebs on Security · October 9, 2026. https://krebsonsecurity.com/2026/10/fbi-arrests-founder-of-ransomware-negotiation-firm/

[23] **FBI arrests another suspected ShinyHunters hacker after agency breach** BleepingComputer · October 9, 2026. https://www.bleepingcomputer.com/news/security/fbi-arrests-another-suspected-shinyhunters-hacker-after-agency-breach/

[24] **Adverse cyber extortions are more common than commonly advised (Q2 2026)** Coveware by Veeam · July 29, 2026. https://coveware.com/2026/07/adverse-cyber-extortions-are-more-common-than-commonly-advised/

[25] **UK police arrest four in connection with M&S, Co-op and Harrods cyberattacks** Reuters via CP24 (reporting the NCA) · July 10, 2025. https://www.cp24.com/news/money/2025/07/10/uk-police-arrest-four-in-connection-with-ms-co-op-and-harrods-cyberattacks

[26] **Threat group profile: DragonForce** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/dragonforce

[27] **Caesars Entertainment says it was also a victim of a cyberattack** NBC News · September 14, 2023. https://www.nbcnews.com/tech/security/caesars-entertainment-says-was-also-victim-cyberattack-rcna105050

[28] **Europol-led crackdown on The Com hackers leads to 30 arrests** BleepingComputer (reporting Europol) · February 27, 2026. https://www.bleepingcomputer.com/news/security/police-crackdown-on-the-com-cybercrime-gang-leads-to-30-arrests/

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions™ SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- LockBit 5.0 returns after Operation Cronos
  More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL	844-974-8669
EMAIL	sales@z7solutions.com
BOOK A CALL	z7solutions.com/book/

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.